

ÜCRETSİZ DERS NOTU ÖZETİ

Bilgi Sistemleri Yönetimi

Bağımsız Denetim Lisansı

Bilgi sistemleri yönetimi ve denetimi

Bu PDF'teki bölüm	6 bölüm
Modüldeki toplam bölüm	37 bölüm
Formül sayısı	1 formül
Son güncelleme	17 Eylül 2026

Bu belge **Bilgi Sistemleri Yönetimi** modülünün ücretsiz bölümlerinden derlenmiştir. Tamamı ve güncel hâli:

<https://www.finlisans.com/ders-notlari/bilgi-sistemleri-yonetimi>

İçindekiler

1. Bilgi Sistemleri Yönetimi ve Stratejik Planlama
2. Bilgi Sistemleri Yönetimi ve Stratejik Planlama • Bilgi Sistemleri Stratejisi, Yönetişimi ve Kurumsal Mimari
3. Bilgi Sistemleri Stratejisi, Yönetişimi ve Kurumsal Mimari • Kurumsal Mimari, Veri Mimarisi ve Kontrol Ortamı Yönetimi
5. Kurumsal Mimari, Veri Mimarisi ve Kontrol Ortamı Yönetimi • Yönetim Fonksiyonları, Roller ve Bilgi Sistemleri Organizasyonu
6. Yönetim Fonksiyonları, Roller ve Bilgi Sistemleri Organizasyonu • Bilgi Sistemlerinde Görevler Ayrılığı, Kaynak ve Risk Yönetimi

Bu PDF, **Bilgi Sistemleri Yönetimi** ders notunun ücretsiz olarak yayımlanan ilk 6 bölümünü içerir. Modülün tamamı 37 bölümden oluşur; kalan 31 bölüm ile soru bankası, sesli anlatım ve deneme sınavları finlisans.com üzerinde yer alır.

Bölümler web sayfasında birbiriyle örtüşecek şekilde hazırlandığı için, bu PDF’te aynı maddenin ikinci ve sonraki tekrarları ayıklanmıştır (183 yinelenen madde). Madde sırası ve bölüm numaraları web sayfasıyla aynıdır.

1. Bilgi Sistemleri Yönetimi ve Stratejik Planlama

Temel Kavramlar

- **Bilgi Sistemleri:** İşletmelerde planlama, kontrol, analiz ve karar verme süreçlerini desteklemek amacıyla veri toplayan, işleyen ve dağıtan; donanım, yazılım ve en kritik unsuru olan insan gücünden oluşan bütüncül sistemlerdir.
- **Bilgi Sistemleri Yönetimi:** Bilgi sistemlerini işletme stratejileriyle uyumlu hale getiren, riskleri yöneten ve kaynakları etkin kullanarak işe değer katmayı hedefleyen, kurumsal yönetimin bir alt kümesi olan süreçler bütünüdür.
- **Misyon:** Bir işletmenin kuruluş amacını, neden var olduğunu, kimlere hizmet verdiğini ve temel faaliyet alanını tanımlayan, kurumsal kimliğin temelini oluşturan ve tüm çalışanlarca bilinmesi gereken yazılı ifadedir.
- **Vizyon:** İşletmenin gelecekte ulaşmak istediği pozisyonu ve rolü ifade eden, genellikle beş yıllık bir zaman dilimini kapsayan ve dış çevre değişimlerine göre belirli aralıklarla güncellenebilen uzun vadeli hedeftir.
- **Strateji:** İşletmenin vizyonuna ulaşmak için izleyeceği, üst yönetim tarafından geliştirilen, kurum kültürünü ve kaynaklarını dikkate alan, ortalama 3 ila 5 yıllık süreyi kapsayan dinamik ve esnek yol haritasıdır.
- **Temel Yetkinlik:** İşletmeye rekabetçi üstünlük sağlayan; müşteri yararı, rakiplerden farklılaşma ve farklı alanlarda uygulanabilirlik özelliklerini bir arada barındıran, stratejinin temelini oluşturan beceriler bütünüdür.
- **Gelişme Vektörü:** İşletmenin etkinlik alanını belirledikten sonra, mevcut veya yeni ürün ve hizmetlerle hangi pazarlara yöneleceğini ve hangi yönde büyüme sergileyeceğini yönetime açıklayan stratejik bir göstergedir.
- **Sinerji:** İşletmenin sahip olduğu araç ve kaynakların hangi alanlarda başarılı olacağını belirleyen, parçaların toplamından daha büyük bir değer yaratılmasını ifade eden stratejik bir öğedir.
- **Bilgi Sistemleri Stratejisi:** Bilgi sistemlerinin işletme hedeflerine nasıl destek vereceğini planlayan, üst yönetimin sorumlu olduğu ve mutlaka genel işletme stratejisiyle tam uyum içerisinde olması gereken fonksiyonel bir stratejidir.
- **Yeşil Bilişim (Green Computing):** Bilgi teknolojilerinin çevreye verdiği zararı en aza indirmek amacıyla enerji tüketimi, atık yönetimi ve doğal kaynak kullanımı gibi alanlarda uygulanan çevreci ve sürdürülebilir bilişim yaklaşımlarıdır.
- **Kurumsal Yönetim:** Şeffaflık ve hesap verebilirlik ilkeleri çerçevesinde, işletmenin hissedarlar, çalışanlar ve müşteriler gibi tüm paydaşlarıyla ilişkilerini düzenleyerek uzun vadeli ekonomik değer yaratılmasını sağlayan kurallar setidir.
- **Fonksiyon Stratejisi:** Kurumsal stratejinin gerçekleşmesine belirli bir birim bazında nasıl destek verileceğini belirleyen, işletme stratejisinden bağımsız belirlenemeyen ve doğrudan ana stratejiye bağlı olan alt planlamadır.
- **Bilgi Sistemleri:** Planlama, kontrol, analiz ve karar vermede kullanılmak üzere bilgiyi toplayan, işleyen, saklayan ve yayan ilişkili unsurlar bütünüdür.
- **İnsan Gücü:** Bilgi sistemlerinin en önemli unsurudur; teknoloji bileşenlerine bütüncül anlam kazandırır.
- **Yönetişim (Kurumsal Yönetim):** Şeffaflık, hesap verebilirlik ve etik değerler çerçevesinde paydaşlara değer yaratmayı amaçlayan kurallar setidir.
- **Misyon:** İşletmenin varlık sebebidir; ne yaptığını ve kime hizmet ettiğini açıklar.
- **Vizyon:** İşletmenin gelecekte kendini gördüğü yerdir; genellikle 5 yıllık bir hedefi kapsar.
- **Strateji:** Vizyona ulaşmak için belirlenen, uzun vadeli, dinamik ve işletmeye özgü yol haritasıdır.
- **Bilgi Sistemleri Stratejisi:** İşletme stratejisine bağlı, bilgi sistemlerinin iş hedeflerine nasıl destek vereceğini planlayan fonksiyonel stratejidir.

Önemli Noktalar

- Bilgi sistemlerinin en önemli unsuru insan gücüdür; insan unsuru çıkarıldığında sistem sadece teknolojik bileşen yığına dönüşür.
- Vizyon belirlenirken ucu açık bir süre yerine, ortalama 5 yıllık bir zaman dilimi hesaba katılmalıdır.
- Stratejik planlar genellikle uzun vadeli olup, işletme literatüründe ortalama 3 ila 5 yıllık bir süreyi kapsamaları beklenir.
- Bilgi sistemleri stratejisinin geliştirilebilmesi için işletme stratejisinin varlığı bir ön koşuldur; BS hedefleri işletme stratejisinin dışına çıkamaz.
- Bilgi sistemleri yönetişiminin temel odak noktası sadece sistemi iyi yönetmek değil, işe 'değer' katmak ve iş birimleri ile BS arasında uyum sağlamaktır.
- Strateji dinamik bir yapıdadır; ekonomik koşullar, teknolojik gelişmeler ve hukuki çerçevedeki değişimlere göre sürekli güncellenmeli ve esnek olmalıdır.
- Bilgi sistemleri yönetişiminin temel vurgusu 'işe değer katmak'tır.
- İşletme stratejisi, bilgi sistemleri stratejisi için bir ön koşuldur ve bağlayıcıdır.
- Bilgi sistemleri stratejisinden nihai olarak Yönetim Kurulu ve üst yönetim sorumludur.
- Strateji 'ne' ve 'ne zaman' sorularına odaklanır, uygulama detaylarını içermez.
- Yeşil Bilişim, çevreye verilen zararı en aza indirmeyi hedefleyen bir kurumsal değerdir.

Sık Yapılan Hatalar

- Stratejiyi sadece BT biriminin sorumluluğu olarak görmek (Aslında üst yönetimin sorumluluğundadır).
- Vizyonu ilelebet değişmez bir metin sanmak (Dış çevreye göre güncellenmelidir).
- Teknik başarıyı (sistemin çalışması), stratejik başarı (işe değer katma) ile karıştırmak.
- Bilgi sistemlerini sadece donanım ve yazılımdan ibaret saymak (İnsan faktörü unutulmamalıdır).

2. Bilgi Sistemleri Yönetimi ve Stratejik Planlama • Bilgi Sistemleri Stratejisi, Yönetişi ve Kurumsal Mimari

Temel Kavramlar

- **Bilgi Sistemleri Stratejisi:** İşletme hedeflerine ulaşmak için bilgi sistemleri önceliklerini belirleyen, kurumsal stratejiye doğrudan bağlı ve üst yönetimin sorumluluğunda olan bir fonksiyon stratejisidir.
- **Fonksiyon Stratejisi:** Kurumsal stratejinin gerçekleşmesine belirli bir birimde nasıl destek verileceğini cevaplayan, bağımsız belirlenemeyen ve doğrudan işletme stratejisine bağlı olan strateji türüdür.
- **Boşluk Analizi:** Bilgi sistemleri stratejisi geliştirme sürecinde, işletmenin mevcut teknolojik durumu ile varmak istediği hedef arasındaki farkların belirlenmesi amacıyla yapılan çalışmadır.
- **Paydaş:** İşletmenin faaliyetlerinden etkilenen veya bu faaliyetleri etkileyen; yatırımcılar, müşteriler, çalışanlar, tedarikçiler ve kamu otoriteleri gibi iç ve dış tüm taraflardır.
- **Yönetişim (Governance):** Günlük işleyle ilgilenen yönetimden farklı olarak, tüm süreçlerin mevcut ve gelecekteki durumlarıyla ilgilenen, üst yönetimin hesap verebilirliğini sağlayan kurallar bütünüdür.
- **Bilgi Sistemleri Yönetişi:** IS kaynaklarının kurumsal hedefleri desteklemesini sağlayan; yapı, süreç ve liderlik unsurlarını içeren, kurumsal yönetişimin ayrılmaz bir parçası olan bütüncül anlayıştır.
- **Bilgi Güvenliği Yönetişi:** İşletmenin bilgi güvenliğine ilişkin yönlendirme ve gözetim faaliyetlerinin üst yönetim tarafından sahiplenildiği, iş operasyonlarının korunmasını amaçlayan süreçtir.
- **Bilgi Sistemleri Yönlendirme Komitesi:** Yönetim kurulu tarafından kurulan, IS yatırımlarını önceliklendiren ve projelerin performansını gözetleyen, teknoloji değil iş odaklı çalışan üst düzey kuruldur.
- **Bilgi Sistemleri Strateji Komitesi:** Çok büyük işletmelerde yönetim kurulu üyeleri ve uzmanlardan oluşan, IS inisiyatifleri hakkında yönetim kuruluna öneri sunan ve yönlendirme komitesine görev veren yapıdır.
- **Bilgi Sistemleri ve İş Uyumu:** Bilgi sistemleri faaliyetlerinin iş hedeflerine katkı sağlaması, teknoloji birimi ile iş birimlerinin aynı dili konuşarak ortak hedefler doğrultusunda hareket edebilmesidir.
- **Kurumsal Mimari:** Kişiler, süreçler, uygulamalar ve teknoloji arasındaki ilişkiyi gösteren, IS altyapısını iş hedefleriyle uyumlu hale getirmek için standartlaştıran bütüncül bir mimari plandır.
- **Veri Mimarisi:** İşletme fonksiyonları incelenerek verinin nereden elde edildiği, nasıl kullanıldığı ve sonuçta nereye iletilildiğinin açıkça tanımlandığı kurumsal mimari alt bileşenidir.
- **Bilgi Sistemleri Stratejisi:** BS'nin iş hedeflerine nasıl katkı sağlayacağını belirleyen, işletme stratejisine bağlı fonksiyonel plan.
- **Bilgi Sistemleri Yönetişi:** BS kaynaklarının kurumsal hedefleri desteklemesini sağlayan bütüncül yapılar, süreçler ve liderlik bütünü.
- **Kurumsal Mimari:** Kişiler, süreçler, uygulamalar ve veri arasındaki ilişkiyi gösteren stratejik yapı ve plan.
- **BS Yönlendirme Komitesi:** BS önceliklerini belirleyen, yatırımları ve projeleri gözetten, yönetim kuruluna rapor veren üst düzey komite.
- **İş Uyumu (Alignment):** Bilgi sistemleri faaliyetlerinin ve hedeflerinin iş birimlerinin hedefleriyle tam örtüşmesi durumu.

Önemli Noktalar

- İşletme stratejisi bağımsız belirlenebilirken, bilgi sistemleri stratejisinin geliştirilmesi için işletme stratejisinin varlığı bir ön koşuldur.
- Bilgi sistemleri stratejisinin başarısından ve gözetiminden, birim yöneticilerinden ziyade yönetim kurulu ve üst yönetim sorumludur.
- IS stratejisi geliştirilirken iş birimi yöneticilerinin, işletme stratejisi geliştirilirken ise IS yöneticilerinin masada olması uyum riski açısından zorunludur.
- Bilgi sistemleri yönetişiminin girdileri varlıklar, insan ve zamanken; temel çıktısı iş hedeflerine katılan değerdir.
- IS Yönlendirme Komitesi teknoloji odaklı bir kurul olmayıp, temel görevi IS-iş uyumunu sağlamak ve kaynak kullanımını gözetlemektir.

Önemli Noktalar

- Kurumsal mimari statik değildir; işletmenin stratejileri veya dış çevre koşulları değiştikçe döngüsel olarak güncellenmesi gerekir.
- Küçük işletmelerde müstakil komiteler olmayabilir ancak görev, yetki ve hedeflerin yazılı olması risk yönetimi açısından şarttır.
- İşletme stratejisi yoksa, bilgi sistemleri stratejisinin varlığı tek başına kurumsal değer yaratmaz.
- Yönetişim (Governance) üst yönetimin sorumluluğundadır ve stratejik yön tayin eder; Yönetim (Management) ise operasyonel uygulamadır.
- Kurumsal mimari statik bir belge değil, çevresel değişimlere göre güncellenen yaşayan bir yapıdır.
- Bilgi güvenliği yönetimi, BS yönetiminin kritik bir alt bileşenidir ve doğrudan iş sürekliliğini korur.
- BS-İş uyumu için teknik terimler yerine 'işe katılan değer' dili kullanılmalıdır.

Sık Yapılan Hatalar

- Hata: Bilgi sistemleri stratejisinin sadece bilgi teknolojileri birimi tarafından belirlenmesi. Doğrusu: Üst yönetim sorumlu olmalı ve tüm paydaşlarca üzerinde anlaşılmalıdır.
- Hata: Yönetim ve yönetişim kavramlarının eş anlamlı kullanılması. Doğrusu: Yönetim günlük işleyişle, yönetişim ise gelecekteki durum ve hesap verebilirlik mekanizmalarıyla ilgilenir.
- Hata: Bilgi sistemleri hedeflerinin 'en iyi' veya 'en hızlı' gibi soyut ifadelerle tanımlanması. Doğrusu: Stratejik hedefler mutlaka ölçülebilir metriklerle belirlenmelidir.
- Hata: Bilgi güvenliğinin sadece teknik bir destek süreci olarak görülmesi. Doğrusu: Bilgi güvenliği, iş operasyonlarının korunması anlamına gelen stratejik bir yönetim unsurudur.
- Hata: Kurumsal mimarinin sadece büyük işletmelerde bulunduğu sanılması. Doğrusu: Her işletmede bir mimari vardır; ancak tanımlanmamış mimariler genelde verimsiz ve karmaşıktır.
- BS stratejisini işletme stratejisinden bağımsız bir 'teknoloji listesi' olarak görmek.
- Yönetişim sorumluluğunu sadece teknik personele (BS birimine) bırakmak.
- Performans ölçümünde sadece teknik metrikleri (hız, kapasite) kullanıp iş etkisini (kâr, verimlilik) göz ardı etmek.
- Kurumsal mimariyi bir kez yapıp bitirilen bir proje olarak algılamak.

3. Bilgi Sistemleri Stratejisi, Yönetiřimi ve Kurumsal Mimari • Kurumsal Mimari, Veri Mimarisi ve Kontrol Ortamı Yönetimi

Temel Kavramlar

- Kurumsal Mimari: İşletmenin bilgi sistemleri altyapısını iş hedefleriyle uyumlu hale getirmek için standartlaştırdığı, strateji gibi işletmeye özgü ve değişen çevre koşullarına göre güncellenmesi gereken bir süreçtir.
- İş Mimarisi: İşletmenin esas işini, misyonunu ve ürünlerini kapsayan; iş birimlerinin amaçlarına ulaşması için uygulanacak temel süreçleri belirleyen kurumsal mimari bakış açısıdır.
- İşlevsel Mimari: İşletmenin ürün veya hizmet üretirken kullandığı uygulamaları ve bu uygulamaların birbirleriyle olan ilişkilerini, iş süreçleri bağlamında tanımlayan mimari katmandır.
- Veri Mimarisi: İşletmenin stratejik veri gereksinimlerini, veri varlıklarını ve veri yönetimi kaynaklarının yapısını tanımlayan; verinin toplanması, saklanması ve dolaşımıyla ilgili kuralları belirleyen modeldir.
- Altyapı Mimarisi: İş süreçlerini ve uygulamaları destekleyen donanım, yazılım ve iletişim altyapısı gibi bilgi sistemleri bileşenlerini belirleyen teknik mimari katmandır.
- Hedef Mimari: İşletmenin vizyonunu gerçekleştirmek için orta vadede (3-5 yıl) ihtiyaç duyacağı bilgi sistemlerini temsil eden, mevcut durumdan ziyade gelecekteki stratejik resme odaklanan tasarımıdır.
- İç Kontrol: Risklerin azaltılması, hedeflere ulaşılması ve yasal uyumun sağlanması amacıyla oluşturulan; işletmenin asıl faaliyetlerine yedirilmiş ve tüm çalışanları kapsayan geniş bir yapıdır.
- Kontrol Ortamı: Üst yönetimin kontrollere yaklaşımını ve etik değerlere desteğini yansıtan; kurum kültürünü ve çalışanların kontrol bilincini şekillendiren iç kontrolün temel bileşenidir.
- Politika: Yönetimin niyetini ve beklentilerini ifade eden, karar alma süreçlerinde çalışanlara rehberlik eden ancak işin detayına girmeyen üst seviye ve sınırlayıcı bir dokümandır.
- Prosedür: Belirli bir işin standartlara uygun şekilde nasıl yapılacağını adım adım tarif eden, süreçlerin tekrar edilebilir ve ölçülebilir olmasını sağlayan kontrol aktivitesi niteliğindeki dokümandır.
- Talimat: Prosedürden daha detaylı olan, uygulama adımlarını yorum gerektirmeyecek netlikte belirleyen ve genellikle kullanılan ekipman veya sisteme yüksek derecede bağımlı olan belgedir.
- Yönetim: Ortak bir hedef doğrultusunda bir grup insanı ve kısıtlı kaynakları; planlama, örgütleme, yönlendirme ve kontrol fonksiyonlarını kullanarak etkin ve verimli şekilde çalıştırma sürecidir.
- Kurumsal Mimari (EA): İş stratejileri ile bilgi sistemleri altyapısını uyumlu hale getirme sürecidir.
- Veri Mimarisi: Kurumsal veri varlıklarının, akışının ve yönetim kurallarının modellenmesidir.
- Kontrol Ortamı: Üst yönetimin kontrollere yaklaşımı ve kurumdaki etik değerler iklimidir (Tone at the top).
- COSO Modeli: İç kontrol için 5 bileşenden (Kontrol ortamı, Risk değ., Kontrol faal., Bilgi-İletişim, İzleme) oluşan çerçeve.
- Politika vs Prosedür: Politika üst seviye ilkeleri, prosedür ise işin nasıl yapılacağını adım adım belirler.

Önemli Noktalar

- Kurumsal mimari projelerinin %66'sı, hedefin iş stratejisinden teknoloji tarafına kayması gibi nedenlerle başarısızlıkla sonuçlanmaktadır.
- Hedef mimari tasarımı, işletmenin 3-5 yıllık orta vadeli planlarını ve vizyonunu esas alarak oluşturulur.
- Veri mimarisi; Kavramsal (iş modeli), Mantıksal (sistem modeli) ve Fiziksel (teknoloji modeli) olmak üzere üç temel katmandan oluşur.
- Kontroller tasarlanırken maliyetin olası faydayı aşmaması esastır; ancak yasal mevzuattan kaynaklanan kontrollerde bu maliyet kriteri aranmaz.
- COSO modeline göre iç kontrol; kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ile izleme ve değerlendirme olmak üzere 5 bileşenden oluşur.
- Kontrol ortamının 'havasını' (tone at the top) belirlemek ve sürdürülebilirliğini sağlamak personelin değil, doğrudan üst yönetimin sorumluluğundadır.

Önemli Noktalar

- Yönetim fonksiyonları genel olarak planlama, örgütleme, yönlendirme ve kontrol olmak üzere dört ana gruba ayrılır.
- Kurumsal mimari durağan değildir; işletmenin faaliyet gösterdiği çevredeki değişikliklere göre düzenli olarak gözden geçirilip güncellenmelidir.
- Kurumsal mimari projelerinin %66'sı başarısız olmaktadır; temel neden iş hedeflerinden kopup teknoloji odaklı hale gelmektir.
- EA dört temel bakış açısıyla incelenir: İş, İşlevsel, Veri ve Altyapı mimarileri.
- Hedef mimari genellikle 3-5 yıllık bir vizyonu kapsar.
- Veri işletmede ortak bir kaynaktır; veri siloları engellenmeli ve ortak bir dil geliştirilmelidir.
- İç kontrol sisteminin merkezinde insan vardır ve her çalışanı kapsar.

Sık Yapılan Hatalar

- Kurumsal mimariyi bir amaç olarak görmek; doğrusu mimari bir amaç değil, işletme hedeflerine ulaşmak için kullanılan stratejik bir araçtır.
- Kurumsal mimariyi sadece bilgi sistemleri biriminin projesi olarak yürütmek; doğrusu iş birimlerinin ve üst yönetimin sürece dahil edilmediği projeler başarısızlığa mahkumdur.
- Süreç ve kontrol kavramlarını karıştırmak; süreç bir işin adım adım tarifiyken, bu adımlar içindeki risk azaltıcı her türlü faaliyet kontrol olarak tanımlanır.
- Politika ve prosedürü aynı hiyerarşide değerlendirmek; politika genel çerçeveyi ve ilkeleri belirlerken, prosedür işin teknik olarak nasıl yürütüleceğini belirler.
- Kontrollerin bir kez tanımlanmasının yeterli olduğunu düşünmek; doğrusu kontrollerin etkinliği denetimle ölçülmeli ve değişen risklere göre periyodik olarak güncellenmelidir.
- Kurumsal mimariyi sadece bir IT projesi olarak görüp iş birimlerini sürece dahil etmemek.
- Kontrol dokümantasyonunu sadece 'uyum' için hazırlayıp güncel ve uygulanabilir tutmamak.
- Mevcut durumu tam analiz etmeden doğrudan karmaşık hedef mimari tasarımlarına geçmek.

5. Kurumsal Mimari, Veri Mimarisi ve Kontrol Ortamı Yönetimi • Yönetim Fonksiyonları, Roller ve Bilgi Sistemleri Organizasyonu

Temel Kavramlar

- **Yönetim:** Ortak bir amaca ulaşmak için insan ve diğer kaynakların planlama, örgütleme, yönlendirme ve kontrol süreçleri aracılığıyla minimum kaynakla ve sürdürülebilir şekilde bir araya getirilmesidir.
- **Planlama:** Yönetimin ilk fonksiyonu olup geleceği tahmin ederek amaçlara ulaşmak için neyin, ne zaman, nasıl ve kim tarafından yapılacağını önceden kararlaştırıldığı eylem planı belirleme aşamasıdır.
- **Örgütleme:** Belirlenen planların hayata geçirilmesi için sorumluluk ve yetkilerin atanması, görev tanımlarının yapılması, organizasyon yapısının kurulması ve kaynakların düzene sokulması işidir.
- **Yöneltme (Yürütme):** Planlanan ve örgütlenen işlere hareket kazandıran, çalışanların motive edildiği, liderlik vasıflarının sergilenerek emir-komuta zincirinin işletildiği ve iletişimin tesis edildiği fonksiyonel aşamadır.
- **Denetim (Kontrol):** Belirlenmiş standartlar ile fiili durumun karşılaştırıldığı, sapmaların tespit edilerek düzeltici tedbirlerin alındığı ve hedeflere ulaşıp ulaşılmadığının ölçüldüğü yönetim sürecidir.
- **Stratejik Planlama:** Üst yönetim tarafından gerçekleştirilen, işletmenin tamamını etkileyen uzun dönemli kararların alındığı ve dış etkenlerin (hukuk, ekonomi, müşteri) izlendiği planlama düzeyidir.
- **Mintzberg'in Karar Verici Roller:** Yöneticinin girişimcilik, sorun çözme (kriz yönetimi), kaynak dağıtıcı ve arabulucu (pazarlık) şapkalarıyla işletmenin geleceğini ve kaynak kullanımını şekillendirdiği roller bütünüdür.
- **Kurumsal Mimari:** İşletme stratejisi ve süreçlerinin teknolojik çözümlerle hayata geçirilmesini sağlayan, özellikle büyük işletmelerde tüm birimlerin katılımıyla oluşturulan bütünsel bir yapılandırma.
- **Sistem ve Ağ Yönetimi:** Sunucu ve ağ sistemlerinin kurulması, yapılandırılması, çalışır halde tutulması ile iş/felaket kurtarma planlarının hazırlanmasından sorumlu olan bilgi sistemleri alt fonksiyonudur.
- **Görevler Ayrılığı (SoD):** Bir işi başlatan, gerçekleştiren ve onaylayan kişilerin farklı olması ilkesine dayanarak hata, ihmal ve suistimal risklerini önlemeyi amaçlayan temel iç kontrol mekanizmasıdır.
- **SoD Matrisi:** Kritik iş adımları ile görev tanımlarının eşleştirildiği, hangi sorumlulukların aynı kişide birleşemeyeceğini gösteren ve personel değişikliklerinde güncellenmesi gereken Excel tabanlı dokümandır.
- **Telafi Edici Kontrol:** Personel yetersizliği nedeniyle görevler ayrılığının uygulanamadığı durumlarda, riskleri önleyemese bile gerçekleştikten sonra fark edilmesini sağlayan (iz kaydı incelemesi gibi) ara çözümlerdir.
- **İz Kayıtları (Log):** Kritik işlemlerde sistemi, tarih/saat bilgisini, yapılan değişikliği ve işlemi yapan tekil kullanıcıyı gösteren, denetim ve telafi edici kontrol amacıyla tutulan asgari verilerdir.
- **Kurumsal SOME:** İkincil düzenlemelerle zorunlu tutulan, siber olaylara müdahale etmekle görevli, genellikle güvenlik veya uyum birimleri bünyesinde yer alan ve hukuk birimiyle koordineli çalışan ekiplerdir.
- **Yönetim Fonksiyonları:** Planlama, Örgütleme, Yöneltme ve Denetimden oluşan temel süreçler.
- **Mintzberg Roller:** Yöneticinin oynaması gereken 10 rol (Kişiler arası, Bilgilendirici, Karar verici).
- **Görevler Ayrılığı (SoD):** Hata ve suistimali önlemek için kritik iş adımlarının farklı kişilere verilmesi.
- **Telafi Edici Kontroller:** Kaynak yetersizliğinde riskleri fark etmek için kullanılan ikincil kontroller (Log inceleme gibi).
- **Kurumsal Mimari:** İş stratejisi ile teknoloji arasındaki uyumu sağlayan yapısal fonksiyon.

Önemli Noktalar

- Yönetim fonksiyonları (planlama, örgütleme, yöneltme, denetim) hem doğrusal hem de birbirini besleyen dairesel bir döngü içinde esnek bir yapıda işletilmelidir.
- Mintzberg'e göre yöneticinin rolleri Kişiler Arası, Bilgilendirici ve Karar Verici olmak üzere 3 ana kategoride toplam 10 rolden oluşur.

Önemli Noktalar

- Planlama türü yönetici kademesine göre değişir: Üst yönetim stratejik, orta kademe taktik, alt kademe ise operasyonel planlama yapar.
- Bilgi sistemleri yönetimi, işletmenin değer zincirindeki yerine göre 'destek noktası' konumundan 'stratejik ortak' konumuna geçerek yeni iş modelleri geliştirmelidir.
- Görev tanımları üst yönetim veya yönetim kurulu tarafından onaylı, yazılı ve personelin kime raporlama yapacağı açıkça belirtilmiş şekilde olmalıdır.
- Görevler ayrılığı ilkesi gereği, yazılım geliştiricilerin üretim (production) ortamına erişimi olmamalı ve sürümler ancak farklı bir çalışanın onayıyla yüklenmelidir.
- Kontrol tasarlanırken temel kriter; kontrolün maliyetinin, maruz kalınan riskin gerçekleşmesi durumunda ortaya çıkacak maliyetten daha yüksek olmamasıdır.
- İz kayıtları (log) asgari olarak; sistemi, tarih/saat/zaman dilimini, değişikliğin ne olduğunu ve ilgili tekil kullanıcıyı/sistemi içermek zorundadır.
- Planlama yönetimin ilk fonksiyonudur ve gelecekteki belirsizliği azaltmayı hedefler.
- Üst yönetim stratejik, orta kademe taktik, alt kademe operasyonel planlama yapar.
- Görevler ayrılığı sadece suistimali değil, hata ve ihmali de önler.
- Log kayıtları asgari; sistem, zaman, değişiklik içeriği ve kullanıcı bilgisini içermelidir.
- Kontrol maliyeti, korunan riskin maliyetini aşmamalıdır.

Sık Yapılan Hatalar

- Yönetimin sadece 'başkalarına iş yaptırmak' olduğunu sanmak (Yöneticinin de kendine has fonksiyonel işleri vardır).
- Görevler ayrılığının işi hızlandıracağını düşünmek (Aksine maliyeti ve süreyi artırır).
- Telafi edici kontrollerin riski tamamen yok ettiğini sanmak (Sadece fark edilmesini sağlar).

6. Yönetim Fonksiyonları, Roller ve Bilgi Sistemleri Organizasyonu • Bilgi Sistemlerinde Görevler Ayrılığı, Kaynak ve Risk Yönetimi

Temel Kavramlar

- **Görevler Ayrılığı:** İş süreçlerini hata, ihmal ve suistimalden korumak amacıyla iş adımlarının farklı çalışanlara bölünmesidir; ancak iş süresini ve personel maliyetini artıran bir unsurdur.
- **Telafi Edici Kontrol (Compensating Control):** Kaynak yetersizliği nedeniyle görevler ayrılığının tam uygulanamadığı durumlarda, hataları önleyemese bile gerçekleştikten sonra fark edilmesini sağlayan ikame mekanizmadır.
- **İz Kayıtları (Log):** Kritik işlemlerde kaydı oluşturan sistem, zaman, değişiklik detayı ve tekil kullanıcı bilgisini içeren, telafi edici kontrol olarak düzenli incelenmesi gereken teknik verilerdir.
- **İş Rotasyonu:** Belirli bir iş adımının geçici olarak asıl görevlisinden farklı birine atanmasıdır; bu yöntem hem süreçteki aksaklıkları tespit eder hem de işletmede iş gücü yedekliliği sağlar.
- **Zorunlu Tatil:** Çalışanın işletmeden bir süre uzaklaştırılmasıyla yerine başkasının bakması sağlanarak, gizli kalmış suistimal veya hataların ortaya çıkarılmasını amaçlayan bir denetim yöntemidir.
- **SoD Matrisi:** Hangi görevlerin birbiriyle çakışmaması gerektiğini gösteren, yönetimce onaylı olması ve sahadaki yetki tanımlarıyla örtüşmesi gereken kritik bir kontrol dokümanıdır.
- **Kaynak Yönetimi:** İnsan, finans, zaman ve teknoloji gibi kısıtlı unsurların, en yüksek örgütsel faydayı elde etmek amacıyla stratejik hedeflere uygun şekilde tahsis edilmesi ve izlenmesi sürecidir.
- **Risk İştahı:** Bir işletmenin hedeflerine ulaşmak için göze alabildiği ve tolere edebildiği azami risk seviyesidir; kurumun yapısına ve sektörüne göre üst yönetim tarafından belirlenir.
- **Risk Kapasitesi:** İşletmenin mevcut finansal, ekonomik ve hukuki ortamı dikkate alındığında, iflas veya büyük zarar yaşamadan alabileceği en üst düzeydeki risk miktarını ifade eder.
- **Riski Azaltma (Mitigation):** Çeşitli kontrol mekanizmaları hayata geçirilerek riskin olasılığının veya etkisinin kabul edilebilir seviyelere düşürülmesi amacıyla en sık tercih edilen risk işleme seçeneğidir.
- **Riski Transfer Etme:** Riskin yarattığı mali zararın sigorta veya dış kaynak kullanımı yoluyla üçüncü taraflara aktarılmasıdır; bu yöntem riskin gerçekleşme ihtimalini değil, sadece sonucunu etkiler.
- **Riski Engelleme (Avoidance):** Kontrollerle kabul edilebilir seviyeye indirilemeyen riskli bir ürün, süreç veya faaliyetin kullanımına tamamen son verilerek riskin kökten ortadan kaldırılmasıdır.
- **Zafiyet (Vulnerability):** Değerli bir varlığın veya sistemin yapısında mevcut bulunan, tehdit unsurları tarafından kötüye kullanıldığında zararlı etki yaratabilecek her türlü zayıflık veya açıktır.
- **En İyi Uygulama Örnekleri (Best Practices):** Bir iş sürecinin etkinliğini iyileştiren, çok denenmiş ve genel kabul görmüş yöntemlerdir; ancak körlemesine değil, işletmenin özel durumuna göre yorumlanarak uygulanmalıdır.
- **Görevler Ayrılığı (SoD):** Hata ve suistimali önlemek için bir iş sürecinin farklı adımlarının farklı kişilere atanması.
- **Telafi Edici Kontroller:** Yetersiz kaynak durumunda görevler ayrılığının yerini tutan (log takibi gibi) ikincil kontroller.
- **Risk İştahı:** İşletmenin hedefleri doğrultusunda kabul etmeye hazır olduğu risk seviyesi.
- **Risk Kapasitesi:** İşletmenin finansal ve hukuki olarak dayanabileceği maksimum risk miktarı.
- **İş Rotasyonu:** Personelin görev yerlerinin değiştirilerek olası hataların veya suistimallerin fark edilmesini sağlayan yöntem.

Önemli Formüller

Risk Değeri Hesaplaması

$$\text{Risk Değeri} = \text{Olasılık} \times \text{Etki}$$

Olasılık: Tehdidin zafiyeti kullanarak gerçekleşme ihtimali • **Etki:** Tehdit gerçekleştiğinde ortaya çıkacak muhtemel zarar veya kayıp

Örnek: Bir sistem sızıntısı olasılığı 3 (orta) ve yaratacağı finansal etki 5 (yüksek) ise, risk değeri 15 olarak puanlanır.

Önemli Noktalar

- Kontrol maliyeti, maruz kalınan riskin gerçekleşme maliyetinden daha yüksek olmamalıdır; ancak yasal zorunluluklar bu maliyet dengesi ilkesinin dışındadır.
- İz kayıtları (log) asgari olarak; sistemi, tarih/saat/zaman dilimini, yapılan değişikliğin içeriğini ve ilgili tekil kullanıcı/sistem bilgisini içermelidir.
- Kaynak planlamasında çalışanların zamanının %100'ünü işe ayıracağı varsayımı hatalıdır; günlük işler ve acil durumlar için mutlaka pay bırakılmalıdır.
- İnsan kaynakları güvenliği için işe alım aşamasında geçmiş araştırması, gizlilik anlaşması ve rekabet etmeme anlaşması olmak üzere üç temel kontrol uygulanmalıdır.
- Risk iştahı sabit değildir; sektördeki değişimler veya işletme stratejisindeki güncellemeler doğrultusunda üst yönetimce yeniden değerlendirilmelidir.
- Risk yönetimi süreci; risk belirleme, risk analizi, risk değerlendirme, risk işleme ve gözetim olmak üzere beş temel adımdan oluşur.
- Görevler ayrılığına ilişkin SoD matrisi ve politika dokümanları en azından bilgi sistemleri yöneticisi tarafından onaylanmış ve tüm personele duyurulmuş olmalıdır.
- Telafi edici kontrollerin (örneğin log inceleme) gözetimi, kritik işi yapan kişiden farklı biri tarafından ve işin niteliğine uygun sık periyotlarla yapılmalıdır.
- Kontrolün maliyeti, koruduğu riskin maliyetinden yüksek olmamalıdır (Yasal zorunluluklar hariç).
- Kaynak planlamasında personelin %100 müsait olacağı varsayımı en büyük hatalardan biridir.
- İz kayıtları (log) asgari olarak sistem, zaman, işlem detayı ve kullanıcı bilgisini içermelidir.
- Bilgi sistemleri yöneticisi teknik personellikten ziyade iş-teknoloji uyumuna odaklanmalıdır.
- Risk yönetimi; Belirleme, Analiz, Değerlendirme, İşleme ve Gözetim adımlarından oluşur.

Sık Yapılan Hatalar

- Hata: Personel sayısı az olan küçük işletmelerde görevler ayrılığı ilkesinden tamamen vazgeçmek. Doğru: Personel kısıtlıysa telafi edici kontroller (log takibi, rotasyon) uygulanarak risk yönetilmelidir.
- Hata: Riski transfer etmenin (sigorta vb.) riskin gerçekleşme ihtimalini ortadan kaldırdığını düşünmek. Doğru: Transfer sadece finansal sonuçların telafisine yöneliktir, olayın gerçekleşme olasılığını değiştirmez.
- Hata: Kaynak planlaması yaparken sadece çalışan sayısını yeterli görmek. Doğru: İnsan kaynağı planlamasında sayı kadar, personelin yetkinlik ve yeterlilik seviyesi de hesaba katılmalıdır.
- Hata: Bir çalışanın üzerinde çok fazla aktif iş olmasını yüksek verimlilik göstergesi saymak. Doğru: Bu durum verimlilikten ziyade bir planlama hatasına veya çıktı kalitesinin düşeceğine işaret edebilir.
- Hata: Risk iştahını birim yöneticilerinin kendi inisiyatiflerine göre belirlemesi. Doğru: Risk iştahı ve kabul edilebilir risk seviyesi, kurumun vizyonu ve stratejisine göre üst yönetim tarafından belirlenmelidir.
- Telafi edici kontrollerin (log inceleme vb.) işi yapan kişi tarafından yapılması (Kontrol zafiyeti yaratır).
- Risk iştahının üst yönetim yerine alt birimler tarafından belirlenmesi.
- Gereklerin hiç değişmeyeceğini varsayarak katı kaynak planlaması yapmak.

Formül Tablosu (hızlı bakış)

Formül adı	Formül
Risk Değeri Hesaplaması	$\text{Risk Değeri} = \text{Olasılık} \times \text{Etki}$

Devamı ücretsiz kayıtle

Bilgi Sistemleri Yönetimi modülünün **37 bölümünün 6 tanesi** bu PDF'te. Kalan 31 bölüm, konu anlatımı ve çıkmış soru tarzındaki soru bankası FinLisans'ta.

- ✓ Ücretsiz üyelikle soru çözmeye hemen başla — kredi kartı istemiyoruz.
- ✓ Tüm SPK/SPL dersleri için ders notu, özet ve formül kartları.
- ✓ Konu bazlı soru bankası, deneme sınavı ve yanlış analizi.
- ✓ Sesli ders anlatımı ile yolda/işte tekrar imkânı.
- ✓ İlerlemeni takip eden panel ve sınav geri sayımı.

Bu modülün güncel ve tam sayfası

<https://www.finlisans.com/ders-notlari/bilgi-sistemleri-yonetimi>

Ücretsiz kayıt ol → <https://www.finlisans.com/auth/signup>

Son güncelleme: **17 Eylül 2026** · Kaynak: finlisans.com ders notları

Bu doküman sınavlara hazırlık amaçlı bir özettir; resmî kaynak yerine geçmez. SPL'nin yayımladığı güncel çalışma notlarını da takip ediniz.